LOTTARE CONTRO UNA FORTEZZA DIGITALE EUROPEA

BANCHE DATI SULLA MIGRAZIONE IN EUROPA E LA POLITICA DELLE FRONTIERE VIOLENTE

LO SCOPO DI QUESTA ZINE

Le frontiere restano centrali nel mantenimento degli assetti globali di potere, con le politiche migratorie al cuore dell'organizzazione degli stati-nazione. Oggi tecnologie sempre più invasive tracciano, identificano, detengono e deportano persone illegalizzate.

L'AI Act europeo, le banche dati biometriche e i droni di sorveglianza mostrano come la tecnologia stia diventando lo strumento principale di una politica migratoria ostile e securitaria.

Mentre gli aeroporti "senza frizioni" promettono viaggi più rapidi per i corpi "desiderabili", aumentano i controlli e le esclusioni per chi fugge da guerre, persecuzioni o eredità coloniali.

Questa zine vuole demistificare la complessità delle tecnologie di frontiera, rendendole visibili e comprensibili per favorire partecipazione, consapevolezza e resistenza alla Fortezza Digitale Europa.

RICERCATRICE

DOTT.SSA PHILIPPA METCALFE

Ricercatrice postdoc ESRC.
Studia come le frontiere digitali e securitarie influenzano la vita delle persone in movimento e delle richiedenti asilo in Europa e nel Regno Unito.

La sua icerca mostra come il controllo e la violenza si trasformino attraverso la tecnologia, rendendo i confini sempre più invisibili ma presenti, dal confine fisico alla vita di ogni giorno.

ARTISTA

RIVER NASH

River è falegname, educatore, artista e designer. Il loro lavoro su questa zine mira a rendere accessibile la ricerca che contiene a chi lotta contro l'ingiustizia delle frontiere violente, sia dentro che fuori i contesti accademici.

LOTTARE CONTRO UNA FORTEZZA DIGITALE EUROPEA:

BANCHE DATI SULLA MIGRAZIONE IN EUROPA E LA POLITICA DELLE FRONTIERE VIOLENTE.

INTRODUZIONE

Questa zine visualizza alcuni degli elementi centrali della Fortezza Digitale Europa: l'infrastruttura digitale che sostiene il regime di frontiera europeo.

L'obiettivo è demistificare tecnologie complesse e opache, rendendole comprensibili e discutibili.
Il regime di frontiera è composto da una molteplicità di controlli e tecnologie:

- respingimenti ai confini,
- uso di droni e sorveglianza per impedire l'ingresso in Europa,
- identificazione biometrica e classificazione delle persone una volta arrivate,
- pratiche violente di detenzione e deportazione,
- criminalizzazione diffusa della mobilità e delle persone in movimento,
- e lunghi tempi d'attesa in sistemazioni inadeguate, in campi o hotel.

Queste tecniche rafforzano politiche ostili ed escludenti, che mirano a controllare, prevenire e scoraggiare la migrazione considerata "indesiderabile" in Europa.
Elemento chiave di questa crescente ostilità è lo sviluppo continuo di banche dati migratorie espansive e interoperabili.
L'UE sta portando avanti un Quadro di Interoperabilità nei settori di frontiere, polizia, asilo e migrazione.

Per interoperabilità si intende la capacità dei sistemi digitali di comunicare e scambiarsi dati tra piattaforme diverse a fini di controllo migratorio.
È importante sottolineare che queste banche dati non colpiscono tutte le persone allo stesso modo: il loro impatto varia in base alla posizione sociale, giuridica e razziale di ciascun individuo.
Le frontiere funzionano così come un sistema di apartheid globale, che stabilisce chi può e chi non può muoversi liberamente.

Questa zine esplorerà tre grandi banche dati migratorie attualmente operative nell'UE:

- Sistema d'Informazione Schengen (SIS II)
- Banca dati europea delle impronte digitali (Eurodac)
- Sistema d'Informazione sui Visti (VIS)

Ispirandosi allo strumento abolizionista ***Algorithmic Ecology*** creato da Stop LAPD Spying Coalition, la zine mappa le ideologie, le istituzioni, gli attori e gli impatti di questi tre sistemi.
Infine, affronta le espansioni imminenti di questa infrastruttura digitale, come parte del nuovo Patto europeo su migrazione e asilo, dove pratiche di sorveglianza e identificazione si stanno diffondendo ulteriormente, aumentando i rischi per il benessere e la sicurezza di chi viene considerato un viaggiatore "rischioso" o "illegale".

***Nota terminologica**

Usiamo il termine persone in movimento piuttosto che "migranti", per porre al centro l'umanità delle persone invece di definirle attraverso una categoria amministrativa.

Allo stesso modo, parliamo di migrante illegalizzato anziché "immigrato illegale", per riconoscere l'illegalizzazione come processo politico imposto da politiche di frontiera ostili. Nessun essere umano è illegale.

DUE CHIACCHIERE PER INIZIARE

Artista:
Ok, ma perché vuoi fare questa zine?

Ricercatrice:
Per me, il punto principale della zine è creare un mezzo accessibile per comprendere infrastrutture digitali di frontiera complesse.

Le tre banche dati che analizziamo (SIS II, VIS e Eurodac) non sono nuove — *Eurodac ha più di vent'anni!* — ma esiste ancora poca consapevolezza su come funzionino, quali impatti abbiano, chi ne tragga profitto e come possano essere contrastate.

Le comunità direttamente colpite conoscono bene questi sistemi, ma le banche dati non sono ancora al centro dell'organizzazione politica, nonostante l'enorme influenza che esercitano.
Il risultato è stata un'espansione massiccia dei controlli di frontiera digitali con poca resistenza al loro sviluppo. A un livello più ampio, ciò ha permesso che l'espansione di "soluzioni digitali" al presunto "problema" della migrazione continuasse con pochissimo scrutinio pubblico.

Certo, esistono lavori straordinari di gruppi e campagne che denunciano l'uso di tecnologie di sorveglianza e identificazione ai confini, ma spesso restano separati dalle lotte contro il razzismo istituzionale e le frontiere violente. Penso che ciò dipenda anche dal fatto che le infrastrutture digitali sembrano invisibili, distanti e troppo tecniche — ed è proprio qui che la zine vuole intervenire.

Artista:
Le persone nell'UE o nel Regno Unito interagiscono con questi sistemi?

Ricercatrice:
Sì e no — dipende se sei cittadino britannico o europeo. In generale, chi appartiene a questi territori subisce meno restrizioni di mobilità e dunque entra meno in contatto con le banche dati migratorie.

Nel Regno Unito, prima della Brexit, chi chiedeva asilo doveva interagire con Eurodac, di solito appena arrivato, quando venivano prese le impronte digitali.

Ironia della sorte, la Brexit ha significato che il Regno Unito non ha più accesso né a SIS II né a Eurodac, riducendo così la capacità di tracciare migranti criminalizzati o di rifiutare la responsabilità per una domanda d'asilo.
Per SIS II, cittadini europei e britannici possono comunque comparire nel database se viene emesso un alert a loro carico da uno Stato membro. Per VIS, invece, l'obbligo riguarda solo i cittadini di Paesi terzi che devono richiedere un visto Schengen.

Dato che il Regno Unito gode di viaggio senza visto verso l'UE, i britannici non interagiscono con VIS — così come altri Paesi con lo stesso privilegio, come USA, Canada o Australia.
Tuttavia, con l'introduzione del nuovo ETIAS (European Travel Information and Authorisation System), anche i viaggiatori senza visto dovranno fornire dati biometrici per entrare nel territorio Schengen.

Questo mostra come tecniche testate su comunità illegalizzate vengano in seguito estese alla popolazione generale, una volta accettate come strumenti "legittimi" di controllo. In questo caso, vediamo l'adozione generalizzata dei controlli biometrici.

Artista:
Chi non ha un approccio abolizionista potrebbe leggere questa zine e pensare: "Ma i criminali non dovrebbero entrare in Europa." Cosa risponderesti?

Ricercatrice:
Direi che dobbiamo stare molto attenti a riconoscere il potere dello Stato di decidere chi è criminale e chi non lo è — e ricordare che questa distinzione può cambiare in qualsiasi momento.
Chiederei anche: cosa rende "criminale" il desiderio di muoversi liberamente, come fanno i bianchi europei?

Le persone in movimento diventano considerate criminali solo perché attraversano frontiere senza un permesso preventivo. Come possono muoversi legalmente se non esistono vie legali per farlo? Questo le rende forse criminali?

In definitiva, credo che nessun essere umano sia illegale.
I veri crimini da affrontare sono l'ordine mondiale coloniale e i regimi di frontiera imposti dagli stati-nazione. So che non tutte e tutti condividono questa prospettiva, ma spero che collegando le grandi ideologie agli effetti concreti sulle persone in movimento, la zine possa mostrare come questi sistemi criminalizzino intenzionalmente comunità razzializzate e storicamente escluse.

QUESTO NON È UN DIFETTO DEL SISTEMA: È IL SUO FUNZIONAMENTO STRUTTURALE.

Artista:
Cosa ti fa pensare che questi sistemi siano razzisti?
Non sono semplicemente necessari per il controllo migratorio, come gli europei che non possono vivere liberamente negli Stati Uniti?

Ricercatrice:
Se prendiamo l'esempio dei "controlli casuali" negli aeroporti europei: quando a essere fermate sono sempre persone razzializzate, non è casuale, è razzismo. Ci sono moltissimi esempi di come i corpi neri e bruni siano stati, e continuino a essere, classificati come rischi per la sicurezza nazionale.

Queste esperienze alimentano i dataset da cui derivano algoritmi e infrastrutture digitali razziste. Un caso emblematico è quello del sistema di streaming dei visti usato nel Regno Unito: un algoritmo classificava le domande secondo un codice a semaforo basato sulla nazionalità.

I Paesi con bassi tassi di approvazione — spesso ex colonie, abitati da persone non bianche — venivano automaticamente segnalati in rosso.
Al centro di questi dibattiti c'è il riconoscimento di chi gode di libertà di movimento e chi no. Tutti, in una certa misura, siamo limitati da nazionalità e passaporti — ma se io voglio viaggiare nel mondo, posso prendere un aereo (magari dopo aver chiesto un visto).
Non dovrò rischiare la vita su una barca sovraffollata, evitando la guardia costiera che vuole respingermi nel Paese da cui fuggo.
Altre persone, invece, affrontano questo ogni giorno.
Per me, è intrinsecamente razzista, crudele e ingiusto.

ECOLOGIA ALGORITMICA

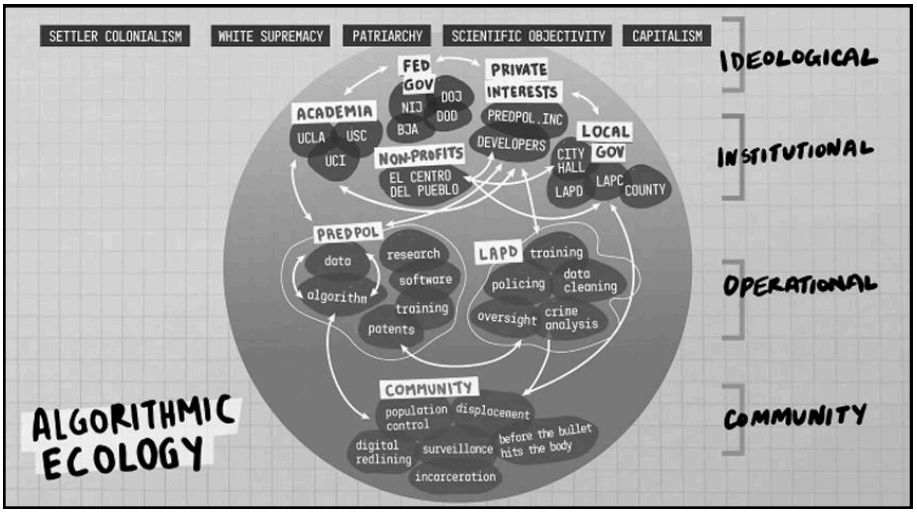
“L’Ecologia Algoritmica non è solo uno strumento analitico, ma uno strumento di resistenza. È uno strumento che mostra che l’abolizione è al tempo stesso necessaria e possibile.”

Questa zine si ispira a *“Algorithmic Ecology: An Abolitionist Tool for Organizing Against Algorithms”* della Stop LAPD Spying Coalition. L’Ecologia Algoritmica è stata usata dalla coalizione come strumento per identificare architetti, attori e persone colpite da un algoritmo di polizia predittiva chiamato PredPol che sostiene di “prevedere” il crimine usando un algoritmo che elabora dati storici sui reati.

L’algoritmo produce aree quadrate di 150x150m per indirizzare gli agenti a pattugliare le zone dove il crimine sarebbe più probabile. I quartieri ricchi raramente sono pattugliati con la stessa tenacia. Così, le comunità iper-poliziate generano dati distorti che alimentano gli algoritmi, causando ancora più polizia, in un circolo vizioso di oppressione classista e razzista sotto la maschera della neutralità.

Le politiche “guidate dai dati” rivendicano spesso obiettività e assenza di bias, ma nel caso di PredPol i dati sono già distorti da pratiche pregresse di razzismo e classismo.

La Stop LAPD Spying Coalition, insieme al collettivo Free Radicals e alla comunità locale, ha mappato le connessioni tra istituzioni, attori politici e interessi economici, arrivando al modello di Ecologia Algoritmica. Lo strumento individua quattro strati: ideologie, istituzioni, operazionalizzazione, comunità. L’intento è esaminare criticamente chi sta dietro dataset apparentemente neutrali.



"L'Ecologia Algoritmica è sia un quadro teorico sia uno strumento organizzativo applicabile criticamente a qualsiasi algoritmo. Questo modello decentra l'algoritmo, osserva i diversi attori che lo plasmano e mostra quali interessi l'algoritmo serva, con l'obiettivo finale di smantellare gli attori che producono danno algoritmico.
È anche un promemoria: dobbiamo esaminare criticamente ciò che si nasconde sotto la 'scientifica' polizia guidata dai dati e andare oltre le critiche centrate solo sulla tecnologia e sui 'dati sporchi'."

Il risultato di questi esercizi di mappatura non è solo visualizzare sistemi complessi, ma anche identificare attori e spazi per intervenire e interrompere: con l'obiettivo di abolire sia le pratiche dannose sia le ideologie che le sorreggono. Inoltre, permettono di capire come gli impatti nocivi sulle comunità siano intrinseci al modo in cui i sistemi sono progettati e usati.
Pur non replicando esattamente l'esercizio proposto dallo strumento, il diagramma qui sotto e le pagine successive mirano a demistificare le tecnologie di frontiera, identificare attori e aziende appaltatrici, e mettere in luce il costo umano per le persone prese di mira dalle banche dati migratorie.

Così, la zine invita a chiedersi cosa vada messo al centro nella lotta contro pratiche (digitali) di confinamento dannose.
Abbiamo adattato il template dell'Ecologia Algoritmica, sostituendo "comunità" con "impatto" per evidenziare la portata e la durata dell'impatto che i controlli di frontiera hanno sulla libertà di movimento. Attraverso visualizzazioni ed esercizi di mappatura, le prossime pagine delineano complessità, ideologie e impatti di tre delle principali banche dati migratorie dell'UE.

Questo testo riassume l'articolo "The Abolitionist Tool for Organizing Against Algorithms"

IL BUSINESS DELLA FORTEZZA EUROPEA

Le ideologie che guidano l'espansione della Fortezza Digitale Europa sono, in larga misura, comuni ai tre database che analizzeremo. Le elenchiamo qui, invitandoti a riflettere su come ciascuna di esse plasmi progettazione, uso e impatti dei sistemi descritti. Riconoscere il ruolo di queste ideologie nel perpetuare controlli di frontiera ostili ed escludenti permette di vedere le strutture di potere più ampie da sfidare oltre il regime di frontiera in sé. Sono queste strutture ad aver prodotto regimi di apartheid della mobilità, che traggono profitto dalla sottomissione delle comunità. Sono queste ideologie che dobbiamo sfidare se vogliamo abolire i controlli di frontiera, digitali o meno.

COLONIALITÀ

Il colonialismo rimanda a pratiche di dominazione, spossessamento, occupazione e sfruttamento di un gruppo su un altro. Tali pratiche sono state alla base della formazione degli imperi europei e continuano a plasmare potere globale e stati-nazione.

La colonialità nomina il perdurare di un ordine mondiale capitalista centrato sull'Occidente. Dentro questo ordine, le strutture sociali e statali sono organizzate secondo pensiero e pratiche coloniali. Ciò influisce su quali corpi sono ritenuti di valore e quali sacrificabili o irrilevanti, determinando chi debba essere escluso tramite i controlli di frontiera. Riconoscere la colonialità come ideologia guida di controlli (digitali) ostili verso migranti illegalizzati e razzializzati mostra la continuità dell'oppressione e dell'esclusione di popolazioni e Paesi colonizzati.

SUPREMAZIA BIANCA

La supremazia bianca si fonda su un'ordinazione gerarchica della razza e sull'idea che la "razza bianca" sia legittimata a mantenere il controllo sulle altre. Questa ideologia modella strutture sociali, economiche e politiche in tutto il mondo, radicando ulteriormente poteri differenziali secondo ordini razzializzati.
I suoi effetti si sentono in frontiere, mobilità, polizia, welfare e nella vita quotidiana, dove aggressioni razziste sono comuni. Si regge sull'idea che le vite bianche contino di più e che la loro sicurezza vada tutelata anche a costo di danneggiare corpi non bianchi. Ciò è evidente, ad esempio, nel genocidio in Gaza, dove i/le palestinesi sono disumanizzati/e; o quando la scomparsa di miliardari bianchi in mega-yacht domina le prime pagine, mentre le morti quasi quotidiane di persone razzializzate alle frontiere marittime europee sono rese invisibili. Le rivolte suprematiste bianche nel Regno Unito (2024), con attacchi a hotel che ospitavano richiedenti asilo, mostrano quanto queste ideologie siano vive oggi.

TECNO-SOLUZIONISMO

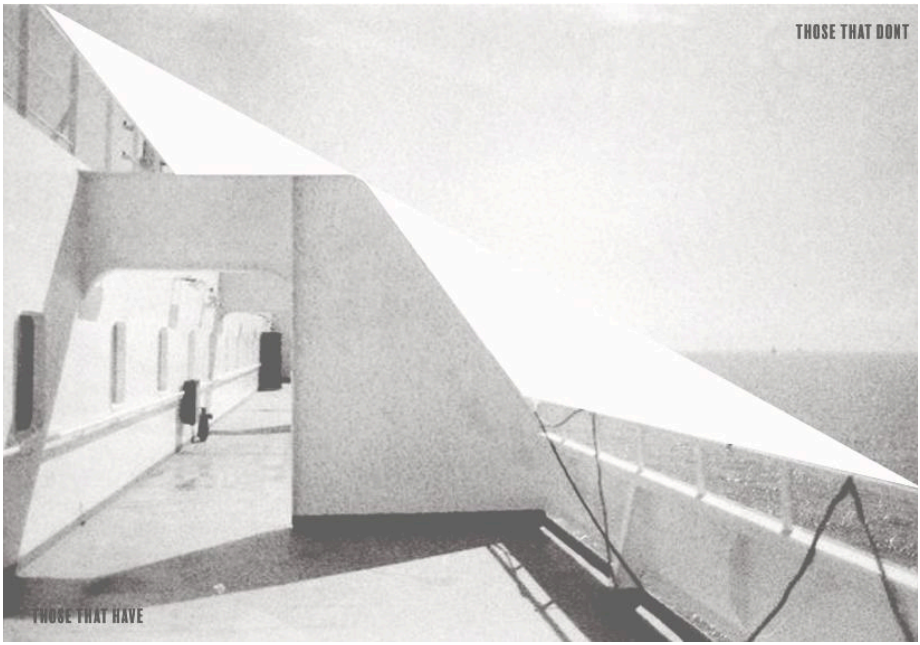
Questa ideologia sostiene che la tecnologia fornisca la soluzione a problemi sociali complessi e sfumati, rappresentandola come neutrale e oggettiva, ignorando storie e bias incorporati nei sistemi che ne plasmano design, uso e impatti.
Si pensi alla polizia predittiva, alimentata da dati prodotti da pratiche di polizia storicamente razziste: gli algoritmi sono più propensi a identificare persone razzializzate come "minacce", perché la polizia ha storicamente preso di mira e arrestato più persone nere (fenomeno documentato in Europa e USA).
Queste "soluzioni" vengono spesso vendute come meno faziose perché spostano la decisione dalle mani umane a quelle di algoritmi presumibilmente neutrali. Così, pratiche violente si rafforzano e si occultano dietro narrazioni di neutralità tecnologica.

CAPITALISMO RAZZIALE

Il capitalismo razziale sostiene che la razza e i processi di razzializzazione siano fondamentali al capitalismo, che fin dall'inizio ha fatto leva su gerarchie tra le persone e sull'estrazione di valore dai corpi razzializzati.

Nella Fortezza Digitale Europa e nelle industrie della sicurezza di frontiera vediamo come il capitalismo razziale informi l'estrazione di profitto dalla continua subordinazione ed esclusione delle persone razzializzate in movimento. Soluzioni di frontiera lucrative sono vendute al prezzo di violenza su questi corpi.

Altri esempi emergono nel complesso carcerario-industriale, dove comunità razzializzate sono disproporzionatamente criminalizzate, e il profitto si ricava da multe, cauzioni e sfruttamento del lavoro carcerario.



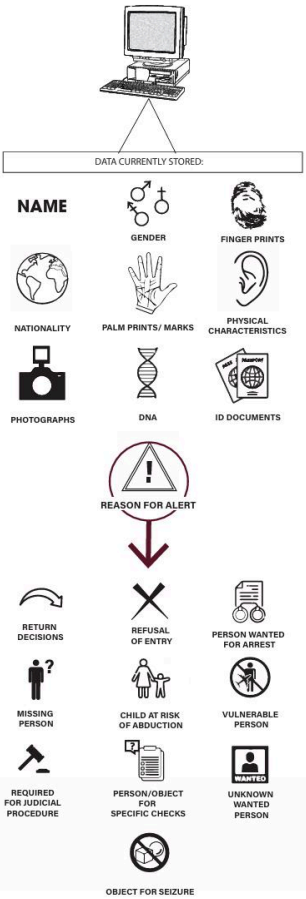
SISTEMA D'INFORMAZIONE SCHENGEN (SIS)

Il Sistema d'Informazione Schengen (SIS II), introdotto nel 1995, è un database centrale per la sorveglianza delle persone considerate "indesiderate" e per la cooperazione di polizia alle frontiere europee, pur aiutando a facilitare la libera circolazione interna nell'UE.

L'ECRIS-TCN consente lo scambio di informazioni tra Stati UE su persone di Paesi terzi con precedenti penali.

Attraverso il SIS II, gli Stati possono emettere alert su chi è considerato una minaccia alla sicurezza, generando divieti di viaggio, controlli o deportazioni.

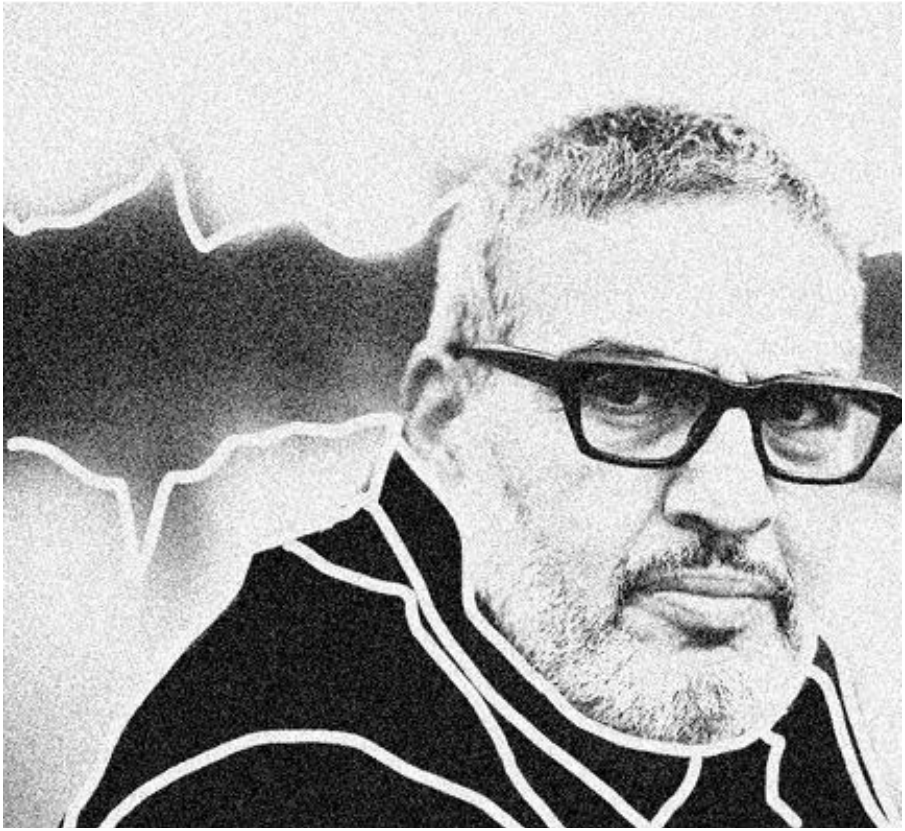
Usato da 30 Paesi, il sistema centralizzato coordina le segnalazioni nazionali (persone, documenti, armi) e nel 2023 ha registrato 15 miliardi di ricerche e 91 milioni di alert, con una crescente enfasi sulla deterrenza della migrazione illegalizzata.



Durata dei dati → Tenuti *"per il tempo necessario a raggiungere lo scopo specifico dell'alert"*. Revisione prevista tra 1 e 10 anni a seconda della tipologia di segnalazione.

Istituzioni → guidato da eu-LISA che collabora con: Consiglio dell'UE, Commissione europea, Parlamento europeo, Garante europeo della protezione dei dati (EDPS), Corte dei conti europea.

Chi colpisce/esiti → può riguardare qualsiasi cittadina/o UE o di Paese terzo per cui sia stato emesso un alert. È usato per applicare divieti Schengen, tracciare, identificare, detenere e deportare.



Esempio:
Il 4 maggio 2024, al Dr. Abu Sittah è stato negato l'ingresso in Francia mentre si recava al Senato per parlare di Gaza. In precedenza, il 12 aprile, gli era stato negato l'ingresso in Germania per un intervento sul suo lavoro medico negli ospedali Al-Shifa e Al-Ahli (ottobre-novembre 2023). Non aveva commesso reati: aveva fornito assistenza medica e intendeva testimoniare. Il divieto è poi stato revocato tramite azione legale. Il caso evidenzia: discrezionalità nell'emissione degli alert; possibile uso politico/abuso del SIS; capacità di criminalizzare ed escludere migrazioni indesiderate; opacità su legittimità e proporzionalità degli alert.

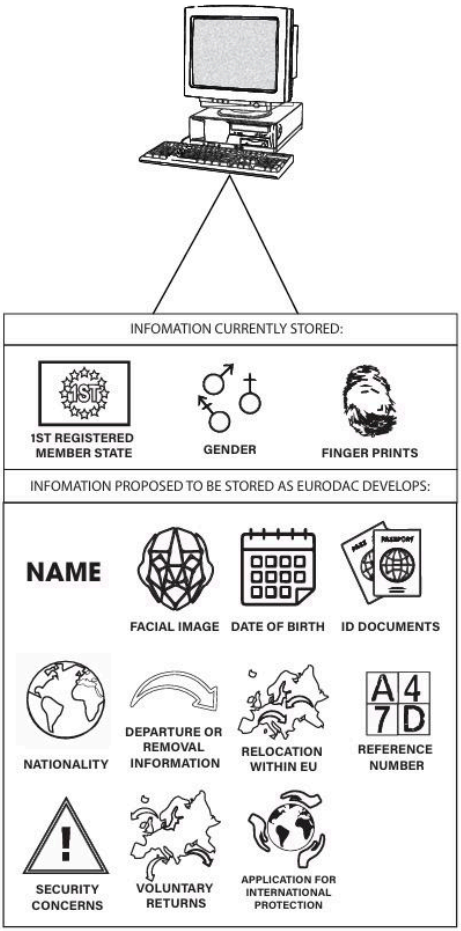
EURODAC

Eurodac è la prima banca dati biometrica paneuropea, introdotta nel 2003. Si concentra su richieste di asilo e mobilità illegalizzata. Il suo scopo è evitare richieste multiple di asilo in più Stati membri, attuando il Regolamento di Dublino (lo Stato di primo ingresso/registrazione è responsabile dell'istruttoria). Nel tempo, lo scopo si è esteso (function creep), ad esempio consentendo accessi di polizia per finalità antiterrorismo e antireato (dal 2015).

Come funziona: raccoglie impronte digitali assegnandole a tre categorie:

- Categoria 1: richiedenti protezione internazionale.
- Categoria 2: ingresso irregolare/non autorizzato.
- Categoria 3: persone trovate illegittimamente presenti nel territorio UE.

Si effettuano ricerche di "hit" per verificare l'identità, mappare gli spostamenti e stabilire se una deportazione verso un altro Stato membro sia giustificabile secondo Dublino.
Cambiamenti imminenti (Patto Migrazione e Asilo, aprile 2024) [7]: grande espansione di uso, finalità e tipi di dati in Eurodac, inclusa l'introduzione della Categoria 4: persone sbarcate dopo operazioni di ricerca e salvataggio. Inoltre Frontex avrà accesso e potrà trasmettere dati al sistema. Nel 2023: 1.776.914 transazioni dati su Eurodac.



Età minima
Attuale: 14 anni. Proposta: 6 anni.

Durata dei dati
- Cat. 1: 10 anni
- Cat. 2: 18 mesi
- Cat. 3: oggi non archiviata; proposta: 5 anni
- Cat. 4 (proposta): 5 anni

Istituzioni
Guidato da eu-LISA, con Consiglio UE, Commissione, Parlamento, EDPS, Corte dei conti.
Contratti
Consorzio S3B (Sopra Steria Benelux – Steria BE, Bull, Gemalto).

Chi colpisce / esiti
- Migranti illegalizzati
- Persone alle frontiere o che le hanno oltrepassate
- Richiedenti asilo
- Persone in movimento

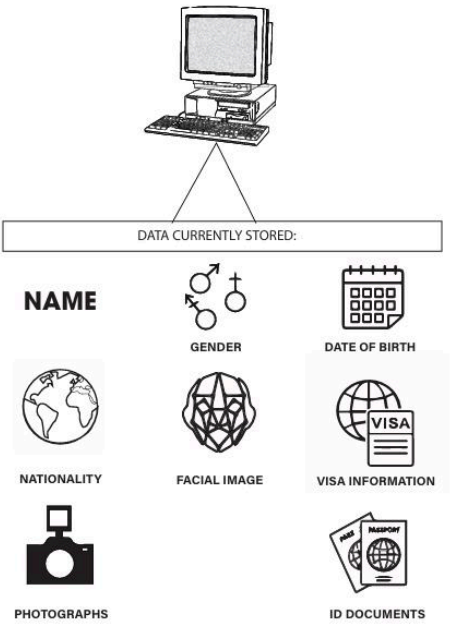
Esempio / questione chiave
Eurodac rende visibile la violenza cui le persone sono sottoposte al primo ingresso in Europa quando chiedono asilo. In condizioni di stanchezza e trauma, vengono raccolti dati cruciali, spesso senza informazione adeguata e senza scelta reale.

Testimonianza di "Saeed" (nome cambiato), passato per Italia e Francia, improntato in entrambi i Paesi prima di arrivare nel Regno Unito: racconta coercizione fisica, minacce di carcere, e la pressione a collaborare per evitare la detenzione.

SISTEMA D'INFORMAZIONE SUI VISTI (VIS)

Il VIS è una banca dati biometrica in uso dal 2011 per permettere alla polizia di frontiera di verificare l'identità di chi entra nello spazio Schengen confrontandola con il visto. Consente la condivisione di dati tra Stati membri con consolati in Paesi terzi (domande, rifiuti, ecc.). I dati inseriti in VIS vengono controllati automaticamente con altri sistemi informativi UE e il sistema utilizza profilazione automatizzata per valutare presunti "rischi" di sicurezza o sanità pubblica.

Inizialmente implementato in alcuni Paesi del Nord Africa, oggi il VIS opera presso tutti i consolati Schengen in Paesi terzi. Rivendicazioni ufficiali: agevolare verifica e rilascio visti, contrastare "visa shopping", individuare documenti fraudolenti, proteggere da furti d'identità, migliorare la sicurezza. Supporta anche l'attuazione del Regolamento di Dublino (tracciando il primo ingresso). In alcune circostanze è accessibile per prevenire/indagare reati. Nato per visti di breve durata, nel 2021 è stato esteso a visti di lungo periodo e permessi di soggiorno. Esternalizzazione della frontiera: il VIS è usato per bloccare a monte l'ingresso di persone considerate a "rischio" di chiedere asilo o sovrastare i tempi del visto.



Ciò rafforza il controllo delle frontiere esterne e si inserisce nell'approccio globale alla migrazione basato sulla cooperazione con Paesi terzi. In pratica introduce uno screening stringente e spesso invalicabile prima di raggiungere la frontiera fisica: un filtro che nega l'ingresso a chi viene prefigurato come potenzialmente "illegale".

Età minima
6 anni (per le impronte digitali: 12 anni).

Istituzioni
Guidato da eu-LISA, con Consiglio UE, Commissione, Parlamento, EDPS, Corte dei conti.

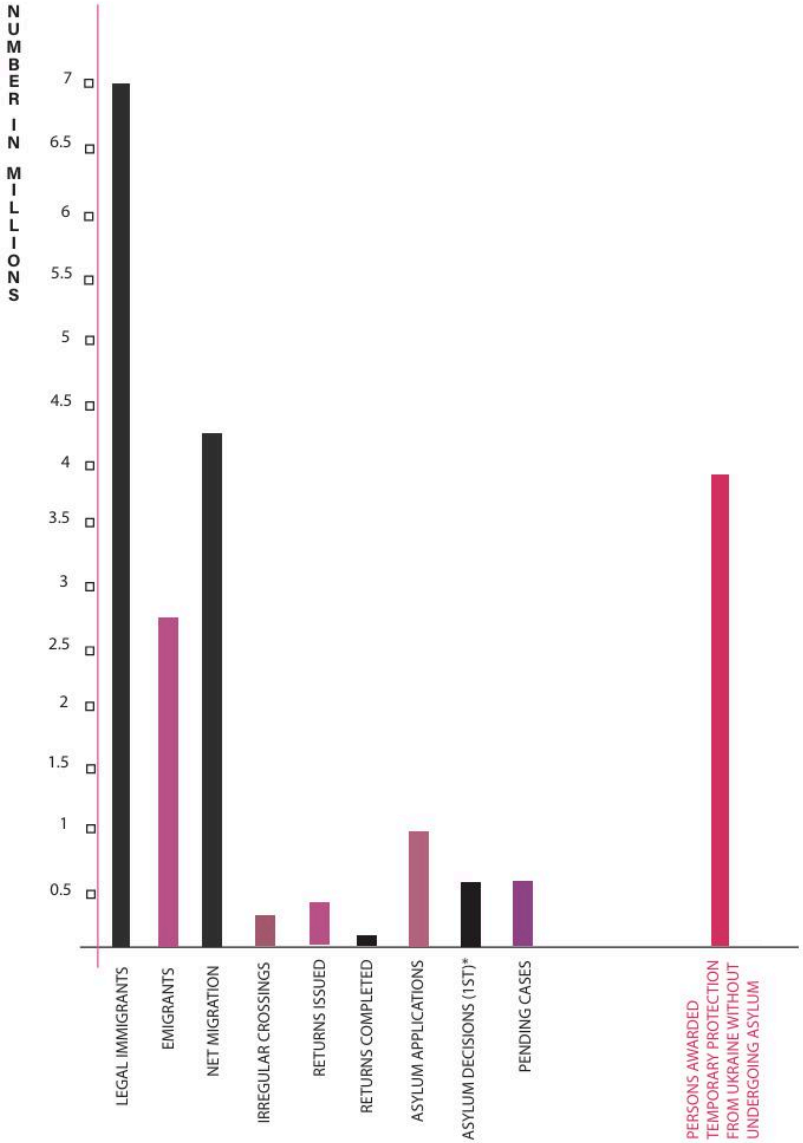
Contratti
- Manutenzione VIS: BRIDGE3 (Accenture NV/SA, Atos Belgium NV/SA, Idemia Identity & Security France SAS).
- Sviluppo VIS + Entry/Exit System + ETIAS: consorzio guidato da Accenture NV, Atos Belgium NV/SA, Idemia Identity & Security France SAS.

Chi colpisce / esiti
Chiunque, cittadina/o di Paese terzo, necessiti di un visto Schengen. L'impatto ricade in misura maggiore su persone razzializzate, dato che molte nazioni imperiali occidentali godono di esenzione visto. Il VIS raccoglie quindi ampie quantità di dati su chi è soggetto a regole restrittive; i visti vengono controllati più severamente, gli overstayer segnalati, e la profilazione espone i corpi razzializzati ad algoritmi che pretendono di individuare "rischi di sicurezza". I dati in VIS possono portare a rifiuti di visti futuri.

Esempio / questione chiave
L'effetto più tangibile è l'inasprimento delle condizioni per ottenere un visto Schengen: diventa più difficile viaggiare in modo sicuro e legale. Un impatto meno discusso è quello economico: il LAGO Collective ha stimato che nel 2023 l'UE ha incassato ~130 milioni di euro solo dai rifiuti di visto (le tasse non sono rimborsabili). Il costo viene quindi scaricato su chi fa domanda, mentre gli Stati traggono profitto dai tentativi di ottenere un visto. Le domande provenienti da Paesi a basso/medio reddito sono più spesso respinte, con i Paesi africani particolarmente colpiti: in pratica, chi ha meno risorse paga di più per poter viaggiare.

Poiché il viaggio senza visto è determinato quasi esclusivamente dalla nazionalità, questa affermazione svela la classificazione preventiva di persone provenienti da determinati Paesi come “rischio di sicurezza”, esattamente come avviene nei sistemi digitali di visti.

Common Identity Depository (CID)
Il CID creerà un deposito unico che accorpa i dati di Eurodac, VIS, EES e ETIAS: i dati saranno confluiti e archiviati in un singolo database. È un tassello chiave per un’Europa digitale interoperabile ed estensiva. Questo sviluppo solleva preoccupazioni: come nota Statewatch, una volta operativo il CID sarà una delle più grandi banche dati biometriche al mondo, con una capacità di almeno 300 milioni di record. Accanto al CID, verrà sviluppato un Multiple Identity Detector per segnalare duplicati presenti tra i database interoperabili, avviando ulteriori verifiche sui dati inseriti e sulle persone cui si riferiscono.

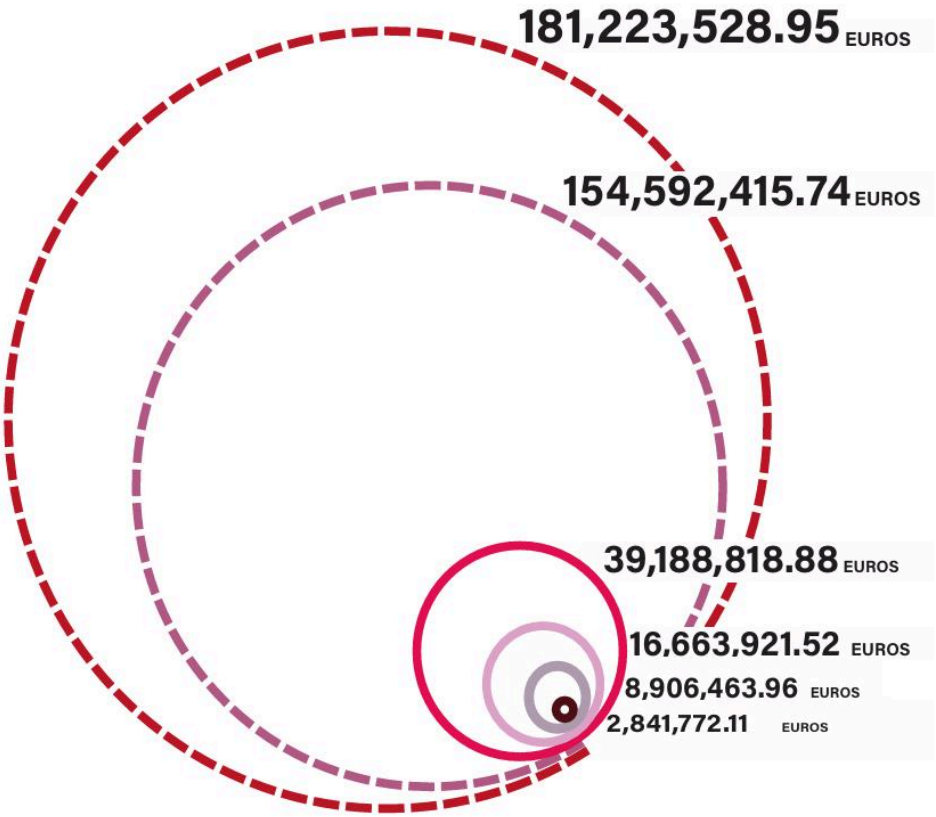


MIGRATION STATISTICS FOR EU (2022)

* Decisione di primo grado indica la decisione emessa dall'autorità competente che agisce come prima istanza amministrativa o giudiziaria nella procedura d'asilo del Paese di accoglienza.

EU LISA CONTRACT - SIS/EURODAC/VIS

TOTAL AWARDED 2018-23:



Information for this graphic was taken from eu-LISA's 'Ex Post Publicity' page:
https://www.eulisa.europa.eu/procurements/ex-post-publicity

CONFINI = CA$H

SVILUPPI FUTURI

Sono in corso sviluppi per rendere ancora più estese le infrastrutture digitali della migrazione e rafforzare la Fortezza Digitale Europa. Tra le novità di banca dati figurano tre sistemi:
Entry/Exit System (EES)

L'implementazione dell'EES è stata rinviata più volte e ora dovrebbe entrare in vigore tra la fine del 2024 o la prima metà del 2025. L'EES sostituirà i timbri sul passaporto per i viaggiatori non UE che entrano nello spazio Schengen. È un sistema informatico automatico che registra quando e dove un cittadino di Paese terzo attraversa il confine UE/Schengen, presentato come strumento per risparmiare tempo a viaggiatori e operatori di frontiera.
Anche eventuali rifiuti d'ingresso precedenti saranno registrati nell'EES.

Obiettivi dichiarati dell'EES: identificare in modo più robusto chi non ha il permesso di entrare o restare nell'UE o chi ha oltrepassato i tempi di soggiorno; prevenire l'uso di documenti fraudolenti; facilitare prevenzione, individuazione e indagine di attività criminali.
European Travel Information and Authorisation System (ETIAS)
Previsto per la prima metà del 2025 (sebbene la data di avvio sia stata rinviata più volte), ETIAS memorizzerà informazioni su chi ha viaggiato senza visto verso l'UE. Sul modello del sistema elettronico statunitense, chi viaggia dovrà inserire i propri dati prima della partenza per richiedere l'autorizzazione a entrare nello spazio UE/Schengen. L'autorizzazione sarà collegata ai documenti di viaggio e durerà tre anni (o fino alla scadenza del documento, se precedente).

Il sito di ETIAS afferma che lo schema di autorizzazione riguarda chi non costituisce un "rischio" di sicurezza per l'UE:
"Questi visitatori hanno ottenuto l'accesso senza visto ai Paesi dell'UE e Schengen in virtù del loro buon curriculum in materia di sicurezza e, pertanto, non sono considerati una minaccia per la sicurezza dell'UE."

IMPA

Questo elenco non è esaustivo: gli impatti della Fortezza Digitale Europea e delle frontiere violente sono vasti. Mettiamo in evidenza alcuni effetti

Esclusione → L'esclusione di determinati corpi dal territorio europeo avviene sia negando l'ingresso sia impedendo la permanenza. Molti sistemi descritti portano all'esclusione di corpi razzializzati, rappresentati come "illegali" o "a rischio" da controllare ed espellere.

Criminalizzazione → La costruzione di sistemi che negano vie legali di viaggio spinge verso percorsi illegalizzati (inclusa la falsificazione di documenti per ottenere un visto), alimentando la demonizzazione delle persone in movimento come "criminali".

Deportazione → Rimozione forzata e violenta dal territorio nazionale. Se Eurodac segnala una impronta in un altro Stato membro, la persona può essere deportata lì per l'esame della domanda d'asilo.

Detenzione → Essere contrassegnati come "illegali" in base allo status migratorio da uno dei database può tradursi in detenzione, una forma di imprigionamento basata sullo status di migrazione, con privazione della libertà.

Viaggi pericolosi forzati → Il diniego del visto impedisce l'uso di rotte sicure (aereo, treni, ecc.). Le persone sono spinte verso barche sovraffollate e insicure, camion, o lunghi tragitti a piedi su terreni pericolosi.

Sfruttamento → L'insic
di lavoro sfruttative (p
rotte sicure comporta
viaggiare illegalmente

ATTO

Divieti di viaggio → Un alert SIS II può imporre un travel ban: impossibilità di imbarcarsi o rischio di arresto/deportazione all'arrivo in aeroporto.

Morte → Migliaia hanno perso la vita nelle traverse pericolose verso l'Europa e dopo le sue frontiere. Non sono rari i decessi in detenzione per violenze o suicidio; anche le malattie a lungo termine, lo stress e la mancanza di cure uccidono. Queste morti sono effetti diretti del sistema.

Mancanza di rotte sicure, rifiuto della ricongiunzione familiare, carenza di documenti → **separazione** di affetti e famiglie attraverso la negazione della libertà di movimento.

Accesso all'asilo → Eurodac può impedire l'accesso all'asilo in uno Stato se si risulta registrati in un altro, generando deportazioni e lunghi ritardi, con impatto su servizi e sostegno disponibili.

Accesso ai servizi essenziali → La criminalizzazione e la difficoltà a ottenere uno status sicuro condizionano l'accesso a sanità e istruzione, spesso vincolati a cittadinanza o status.

curezza dello status espone a condizioni
aghe più basse, ricatti). L'assenza di
costi esorbitanti per viaggi pericolosi:
costa molto più che prendere un aereo.

Malessere e salute → Oltre ai limiti di accesso alla sanità, lo stigma e l'ostracismo producono stress cronico, crisi di salute mentale, evitamento dei medici per timore di controlli, con effetti fisici e psicologici profondi.

WE TOO HAVE LIVES TO LIVE

RESISTENZE

Esistono molte forme di resistenza alla Fortezza Digitale Europea, sia da parte di chi subisce la violenza di frontiera sia di chi agisce in solidarietà. Alcune forme puntano direttamente la tecnologia, altre trovano modalità non tecnologiche. Le pratiche vanno dal continuare a muoversi (nonostante i controlli) a azioni legali che denunciano gli aspetti discriminatori e razzisti dei controlli dataficati. Di seguito alcuni esempi (non esaustivi).

DA PARTE DELLE PERSONE IN MOVIMENTO

Bruciare le impronte → Pratica documentata per evitare la scansione e l'aggancio nelle banche dati. È un atto di autolesione come rifiuto dell'estrazione biometrica, che mostra l'estremo livello di violenza insito nei controlli digitali e la spinta a scelte drastiche per evitare conseguenze come la deportazione.

Continuare a muoversi → Nonostante impronte in Eurodac (es. prese in Grecia) e rischio di deportazione, proseguire verso altre mete (es. Germania) rifiutando regole che negano la libertà di movimento. È una forma potente di disobbedienza quotidiana.

Appropriazione di mobilità contro i visti biometrici → Come analizza Stephan Scheel, le persone trovano spiragli dentro i sistemi biometrici del VIS tramite "documenti davvero falsi" (real fake): ad esempio, ottenere un contratto reale per un lavoro fittizio per superare il processo di visto, o prendere in prestito denaro per mostrare sufficienti risparmi e restituirlo dopo il rilascio del visto. Anche di fronte al rafforzamento biometrico, le persone praticano il proprio diritto alla mobilità.

DA PARTE DI CAMPAGN* E PROFESSIONIST*

#ProtectNotSurveil → Coalizione di gruppi per i diritti di migranti e diritti digitali attiva lungo tutto l'iter dell'AI Act.

Quattro richieste chiave:

a. Vietare pratiche di IA dannose nel contesto migratorio;
b. Regolare tutti i sistemi di IA ad alto rischio nella migrazione;
c. Applicare l'AI Act alle grandi banche dati migratorie dell'UE;
d. Rendere l'AI Act un strumento di tutela, non di sorveglianza.

Azione legale contro l'algoritmo di "visa streaming" nel Regno Unito. Il gruppo Foxglove, con il Joint Council for the Welfare of Immigrants (JCWI), ha promosso un'azione legale contro un algoritmo che smistava le domande di visto per nazionalità, prendendo di mira persone razzializzate. Poco prima dell'udienza (agosto 2020), l'Home Office ha dichiarato che avrebbe interrotto l'uso dell'algoritmo: un risultato che, pur evitando il giudizio in tribunale, ne ha impedito la prosecuzione.

Rendere visibili lobbying e profitti. Ricerche di *Statewatch, TNI, Corporate Watch, Privacy International* documentano il ruolo di attori privati nella progettazione/implementazione dei controlli digitali e di sicurezza alle frontiere, nominando grandi aziende tecnologiche e degli armamenti al centro del sistema europeo.

Questo fornisce indicazioni preziose su chi indirizzare con pressioni pubbliche o boicottaggi.

Resistenze nel sistema sanitario (UK) → Campagne come *Docs Not Cops e Patients Not Passports* si oppongono alla condivisione dei dati tra ospedali e Home Office, che porta a controlli sullo status migratorio dei pazienti. Queste pratiche creano paura e spingono molte persone a evitare le cure per timore di retate o deportazioni.

Le campagne informano il personale sanitario e chiedono la fine di queste politiche. Anche lavoratori del NHS hanno protestato contro Palantir, coinvolta in tecnologie di sorveglianza militare usate da Israele contro i palestinesi.

COPYRIGHT BRUTTO,
POICHÉ BRUTTO SEMPRE.

MA SPECIALMENTE,
A MAGGIOR RAGIONE LA SERA... NO!